

ORIGINAL

UNITED STATES DISTRICT COURT

for the
Central District of California

15 - 1676M

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address)) Case No.
 Information associated with the account identified as)
 jacksoncyh@yahoo.com that is stored at premises)
 controlled by Yahoo!, Inc., located at 701 First Avenue,)
 Sunnyvale, California 94089.)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
 (identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit is incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

You must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

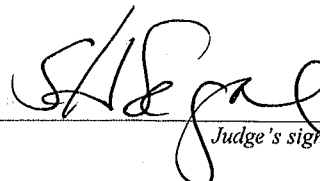
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

(name)

IT IS FURTHER ORDERED that the Provider named in Attachment A shall comply with the further orders set forth in Attachment B, and shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant.

Date and time issued:

9/8/15 2:37pm


 Judge's signature

City and state: Los Angeles, California

Suzanne H. Segal, U.S. Magistrate Judge
 Printed name and title



AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.: 15-1676 M	Date and time warrant executed: 09/08/15 11:25 AM (PT)	Copy of warrant and inventory left with: Custodian of Records
-------------------------------	--	---

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

**Yahoo! Inc. provided one compact disc (CD)
containing e-mails and account information.**

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: **11/13/15**

Bennett Hong
 Executing officer's signature
Bennett Hong Special Agent
 Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account identified as jacksoncyh@yahoo.com that is stored at premises controlled by Yahoo!, Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, CA 94089.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE

1. The search warrant will be presented to personnel of Yahoo!, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the agent who serves the search warrant.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). In conducting this search, the

search team shall take notes regarding how it conducts the search.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 60 days from the date of receipt from the PROVIDER of the response to this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 60-day period.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, from account creation to present, including:

i. All e-mails associated with the SUBJECT ACCOUNT, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, and deleted e-mails, as well as all header information associated with each e-mail, and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books,

contact and buddy lists, calendar data, pictures, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations.

c. Any and all cookies used by any computer or web browser associated with the SUBJECT ACCOUNT, including the dates and times associated with the recognition of any such cookie;

d. All subscriber information pertaining to any other account accessed using any of the same cookies that have been used to access the SUBJECT ACCOUNT (and identified above in paragraph II.10.c), including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of

service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1030(a)(2)(c), (a)(4) (Unauthorized Access to Computer and Obtaining Information, with Intent to Defraud), 18 U.S.C. §§ 1343, 1344 (wire and bank fraud) and 18 U.S.C. § 1028A (aggravated identity theft), namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts;

ii. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;

iii. Information related to the access of bank accounts in names other than the subscriber of the SUBJECT ACCOUNT;

iv. Information relating to wire transfers and other bank transactions;

v. Information relating to IP address:
71.199.215.24 or Travelodge;

vi. Information relating to computer programs or software that can be used to obtain or secure unauthorized access to a computer or computer network, including the actual use, development, or operation of such programs or software;

vii. Information relating to Elite Professional Corporation ("Elite"), East West Bank Länsförsäkringar Bank or Nordjyske Bank;

viii. Information related to any Elite employee including but not limited to ZHU;

ix. Information relating to the results or effects of any unauthorized computer access, including deleting or overwriting files, exfiltrating or transferring data, evading detection, warnings or messages to victims conveyed by means of such access, or other damage, theft, or loss resulting from such access;

x. Information relating to any files, information, folders, or other data taken from the computers, networks, e-mails, or any other information owned or maintained by Elite;

xi. Information relating to communications between the SUBJECT ACCOUNT and other persons, accounts, or computers that involve unauthorized access of protected computers, including but not limited to unauthorized access into computer systems as well as to any individuals or computers that may be controlling or participating in the unauthorized access, to include computer logs, personal messages, and/or e-mail related to the unauthorized access;

xii. Information relating to explaining or illustrating methods for gaining access to computers or computer networks, including how to configure or use computer hardware, software, or other related items for purposes of gaining access to computers and/or computer networks;

xiii. Information relating to the identity of any person using an e-mail account that was the sender or recipient of any e-mails seized pursuant to any of the categories above;

b. All records and information described above in Sections II.10.b, II.10.c, and II.10.d.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

BENNETT HONG
11000 WILSHIRE BOULEVARD, SUITE 1700
310-996-3836 (FAX)
bennett.hong@ic.fbi.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

14. IT IS FURTHER ORDERED that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant.

AFFIDAVIT

I, Bennett Hong, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I received a B.A. in both Economics and East Asian Studies from the University of California, Los Angeles in 2002, and an M.A. in Negotiation, Conflict Resolution and Peacebuilding from California State University, Dominguez Hills in 2007. I was employed as a U.S. Customs and Border Protection Officer from 2002 to 2005, and an Investigative Specialist with the Federal Bureau of Investigation ("FBI") from 2005 to 2008. I am a Special Agent ("SA") with the FBI, and have been so employed for approximately six years. I am currently assigned to the Los Angeles Field Office, where I specialize in the investigation of computer and high-technology crimes, including computer intrusions, denial of service attacks and other types of malicious computer activity. During my career as an FBI SA, I have participated in various computer crime investigations as well as national security investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology.

2. I make this affidavit in support of an application for a search warrant for information associated with the account identified as jacksoncyh@yahoo.com (the "SUBJECT ACCOUNT") that

is stored at premises controlled by Yahoo!, Inc. (the "PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 701 First Avenue, Sunnyvale, CA 94089.¹ The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d) to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

¹ Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

3. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNT constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. §§ 1030(a)(2)(c), (a)(4) (Unauthorized Access to Computer and Obtaining Information, with Intent to Defraud), 18 U.S.C. §§ 1343, 1344 (wire and bank fraud) and 18 U.S.C. § 1028A (aggravated identity theft).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF INVESTIGATION

5. The FBI is investigating fraudulent wire transfer requests related to the unauthorized access to e-mail accounts affiliated with an employee of Elite Professional Corporation ("Elite"). The employee was an Elite Financial Advisor with power of attorney over the accounts of a client. The employee's Yahoo! business e-mail accounts were compromised and were used

to send two fraudulent requests to transfer money from the victim-client's bank account to accounts overseas. One of the two fraudulent wire transfer requests was successful and \$69,000 was stolen from the victim-client. The SUBJECT ACCOUNT is one that was fraudulently created in the victim-client's name to facilitate the scheme.

III. STATEMENT OF PROBABLE CAUSE

6. On or about April 23, 2015, the FBI received a complaint from Katie Zhu ("ZHU"), who is an employee of Elite located in the City of Industry, CA. During this and in a subsequent interview with the FBI, ZHU provided the following information, which I know about through reading FBI reports of these contacts:

a. Jackson Yen Huang ("HUANG") is an Elite client and ZHU is HUANG's Elite financial advisor and handles HUANG's finances. Elite has a power of attorney over aspects of HUANG's finances and as such, ZHU is authorized to make wire transfers on HUANG's behalf to different business ventures.

b. HUANG was the victim of wire fraud. Specifically, on or about April 08, 2015, a fraudulent wire transfer in the amount of \$69,000 was processed, drawing funds from one of HUANG's bank accounts with East West Bank, 379 South Diamond Bar Boulevard, Diamond Bar, CA 91765, and was transferred to an account at Länsförsäkringar Bank in Sweden, held under the name of "Raafat Tawadrous."

c. On or about April 21, 2015, a second fraudulent wire transfer in the amount of \$90,000 was initiated but was canceled due to a lack of sufficient funds in HUANG's bank account. The wire transfer was slated to go to a bank account in Denmark at Nordjyske Bank, held under the name of Emma Zimoh.

d. ZHU found out about the fraudulent wire transfers on or about April 21, 2015, after talking to an East West Bank representative, Samsonz Lam ("LAM"). LAM called ZHU to advise her that HUANG's account did not have sufficient funds to cover the \$90,000 wire transfer to Denmark, which ZHU had supposedly requested via e-mail earlier in the day. ZHU informed LAM that she did not authorize any wire transfer requests in the amount of \$90,000 nor did she send LAM any e-mails regarding such.

e. ZHU further discovered that on or about April 06, 2015 (later determined to actually be April 08, 2015), an e-mail from her work account, katie@eliteppp.com, was sent to East West Bank requesting a wire transfer for HUANG in the amount of \$69,000 to a bank in Sweden. Ryan Lo ("LO"), a customer service representative at East West Bank, sent a reply to katie@eliteppp.com (ZHU's same genuine e-mail account) requesting more information from HUANG. A response to that request was sent from the SUBJECT ACCOUNT to katie@eliteppp.com, which was then forwarded on to LO (This created an e-mail string making it appear as though HUANG had authorized ZHU to wire the money because the SUBJECT ACCOUNT (jacksoncyh@yahoo.com) contained HUANG's first name (Jackson), and middle and last initials.) ZHU had not actually participated in any parts of

the e-mail conversation and did not authorize anyone else to use her e-mail account. According to ZHU, HUANG was also not aware of the wire transfer requests and did not initiate or authorize them.

7. On May 13, 2015, I reviewed copies of the e-mails between the SUBJECT ACCOUNT, katie@eliteppp.com, LAM and LO, that ZHU provided to the FBI. Additionally, on the same day, I received copies of the same e-mails from Jenny Mooc, Risk Management Supervisor, Risk & Operations Department, at East West Bank. A review of the e-mails confirmed ZHU's report regarding the e-mails.

8. On July 01, 2015, I learned from records obtained from the PROVIDER that the SUBJECT ACCOUNT was created on April 08, 2015 (the same day as the first fraudulent wire transfer request) from the IP address 71.199.215.24. The same records indicated that the account was still active but that no login activity was logged since the account was created. A "WhoIs" query of the IP address revealed that it was registered to Comcast.

9. On July 17, 2015, I learned from records obtained from Comcast that for the relevant time period the IP address 71.199.215.24 resolved to a Travelodge located in Okeechobee, Florida. Also, on July 17, 2015, I called a publicly listed phone number for the Okeechobee Travelodge and spoke with "Varun" (Last Name Unknown), who told me that he was the manager of the Travelodge. Varun indicated that the Wi-Fi internet service at his Travelodge was complimentary and unsecured

(required no password), and that one did not have to be a paid guest at the hotel to utilize the connection. In addition, Varun referred me to the hotel's Wi-Fi management company. I spoke to a representative of that company who informed me that no logs of user activities were kept.

10. On May 13, 2015, I was forwarded a copy of a notification ZHU had received from the PROVIDER regarding a suspicious login attempt to her e-mail account katie elite@yahoo.com. The notification advised that on April 09, 2015 at 4:33AM GMT+8 (the same day as the first fraudulent wire transfer when adjusted for the time zones) someone tried to sign in to the aforementioned e-mail account from an unrecognized device in Singapore.

11. On May 28, 2015 and on June 01, 2015, I learned from records obtained from the PROVIDER that the e-mail accounts of katie elite@yahoo.com and katie@eliteppp.com were one and the same. The latter e-mail account was a business account hosted by the PROVIDER but was linked to the former account as hosted by the PROVIDER. Thus, e-mails that were sent and/or received, were mirrored in each account.

12. A review of the records also did not reveal any account logins on April 8, 2015, which, as discussed above, was the date of the fraudulent e-mail string was transmitted from the SUBJECT ACCOUNT to a representative of East West Bank.

13. Based on my training and experience, discussions with other law enforcement officers, and a conversation with a Yahoo! representative, I know that the lack of login activity does not necessarily mean that the account was inactive for that period. In fact, the fraudulent e-mails sent from the account show that it was being used despite the lack of logins. The lack of logins may be due to the fact that the account was continuously logged into since creation; alternatively, it may be due to the fact that the user accessed the account through a mobile application.

14. Other than what has been described herein, to my knowledge the United States has not attempted to obtain the contents of the SUBJECT ACCOUNT by other means.

IV. BACKGROUND REGARDING E-MAIL AND THE PROVIDER

15. In my training and experience, I have learned that the PROVIDER provides a variety of online services, including e-mail, to the public. The PROVIDER allows subscribers to obtain e-mail accounts at the domain name www.yahoo.com, like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with the PROVIDER. During the registration process, the PROVIDER asks subscribers to provide basic personal information. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as

account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

16. A subscriber of the PROVIDER can also store with the PROVIDER files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an e-mail account may be found in such information.

17. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

18. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNT.

19. In my training and experience, e-mail account users will sometimes communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the

communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

20. I know from my training and experience that the complete contents of an e-mail account may be important to establishing the actual user who has dominion and control of that account at a given time. E-mail accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which e-mail accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an e-mail account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore,

the contents of a given account, including the e-mail addresses and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with the SUBJECT ACCOUNT for review by the search team.

21. Because two of the primary purposes of the investigation at this point are to identify the individual(s) responsible for the business e-mail compromise and to determine the scope of the scheme, I request that the PROVIDER provide the entire content for the SUBJECT ACCOUNT since inception (April 08, 2015) until the time the requested warrant is served on them, and that the items to be seized set forth in detail below permit law enforcement to seize such items without limit as to time in order to assist in identifying the individuals participating in this scheme and the scope of their activities.

22. Further, because the SUBJECT ACCOUNT appears to have been created for the specific purpose of committing fraud and the account was created the same day it was used to send a fraudulent e-mail in furtherance of the criminal activity, I am requesting the entire contents of the account without a date range restriction.

23. Relatedly, the government must be allowed to determine whether other individuals had access to the SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an e-mail account, that small subsection might give the misleading impression that only a single user had access to the account.

24. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of e-mail conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an e-mail or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an e-mail account by law enforcement personnel with information regarding the identified criminal activity, subject to the search

procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

25. Based on my training and experience, I also know that networks and hierarchies of individuals involved in hacking and computer intrusions are often extensive and have many layers. Often times certain individuals involved in acquiring the information or directing its acquisition may not be actively engaged in directing a particular step of the procurement, but are kept informed, often by receiving or sending carbon copies ("cc's") from or to others on e-mail communications. In order to fully identify the extent and nature of the network--and thus the conspiracy--it is important to obtain e-mail communications that may not show participation by the user of a particular account, but that will help identify that person and their role in the network.

26. I also know that a user's e-mail account can include photographs or other notes in the contact list or address book regarding people with whom the user is in contact, information that is either automatically imported from social media sites, or data or files actively entered by the user of the e-mail account. Therefore, I request authority to seize documents related to the identity of the user of any e-mail account included on communications relevant to the computer intrusion and attack described herein.

27. In part for that reason, the requested e-mail search warrant specifically requests any and all logs of user activity, including web requests or HTTP request, web server logs, web access logs, login tracker logs, account management logs, web proxy logs, and any other information concerning web sites navigated to or analytics related to the SUBJECT ACCOUNTS. Furthermore, those records can show other actions taken in furtherance of the conspiracy, such as whether the user used Yahoo!, the PROVIDER, to run queries (for example, to identify personnel to whom he would send the e-mail, or other online reconnaissance in preparation for the attack), or other accounts logged into by the user.

28. In order to identify other accounts used or maintained by the user of the SUBJECT ACCOUNT, the warrant also calls for the PROVIDER to disclose any cookies associated with the SUBJECT ACCOUNT, i.e., those cookies in place on any computers or web browsers (for example, Internet Explorer or Google Chrome) used to access the SUBJECT ACCOUNT. The warrant also calls for the PROVIDER to identify any other accounts accessed by any computer or web browser using the same cookies. Such accounts may be other e-mail accounts, document storage accounts, or social media accounts.

29. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original

production from the PROVIDER under seal until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for the PROVIDER to authenticate information taken from the SUBJECT ACCOUNT as its business record without the original production to examine. Even if the PROVIDER kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the PROVIDER to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the PROVIDER to examine a particular document found by the search team and confirm that it was a business record of the PROVIDER's taken from the SUBJECT ACCOUNT.

b. I also know from my training and experience that many e-mail accounts are purged as part of the ordinary course of business by providers. For example, if an e-mail account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an e-mail account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her e-mail account. Preserving evidence,

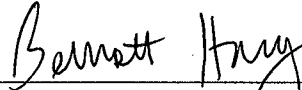
therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

V. REQUEST FOR NON-DISCLOSURE

30. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscriber(s) of the SUBJECT ACCOUNT, of the existence of the warrant because there is reason to believe that such notification will result in: (1) flight from prosecution; (2) destruction of or tampering with evidence; (3) otherwise seriously jeopardizing the investigation; or (4) unduly delaying trial. The details of the current investigation set forth above are not public, and I know, based on my training and experience, that persons engaged in unauthorized access, intrusions and fraud will destroy digital evidence if they learn of an investigation. In addition, if the PROVIDER notifies the target(s) of the investigation that a warrant has been issued for the SUBJECT ACCOUNT, the target(s) might further mask their activity and seriously jeopardize the investigation.

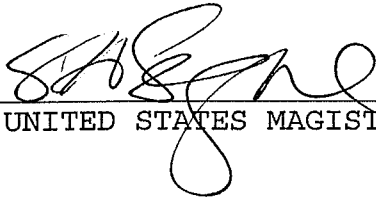
VI. CONCLUSION

31. Based on the foregoing, I request that the Court issue the requested search warrant.



BENNETT HONG, Special Agent
FEDERAL BUREAU OF INVESTIGATION

Subscribed to and sworn before me
On September 8, 2015.



UNITED STATES MAGISTRATE JUDGE